# Technology Approaches to Currency Security

**John C. Murphy, Daniel Dubbel, Richard Benson**

**The Johns Hopkins University**
**Applied Physics Laboratory**
**Johns Hopkins Road**
**Laurel, MD 20723**

## ABSTRACT

The continued development of reprographic technology and computer graphics (notably color laser copiers, scanners and color laser printers) has increased the tools available to both professional and casual counterfeiters. The result is an increase in the counterfeit risk to the U.S. dollar and other currencies. To counter these threats improved methods of currency authentication are needed both for use by the general public and by national currency authorities. The growing number of cash transfer machines has increased the importance of machine readable security features. This paper describes some technology based approaches to currency security based on special materials. It also proposes a metaphor for currency authentication which attempts to provide a framework for unifying approaches based on secure features and those based on codes.

**Keywords**: counterfeit, currency, deterrence, authentication

## 1.0 INTRODUCTION

The new reprographic technology increases the counterfeiting threat in several ways. First, the professional counterfeiter and potentially the state-supported counterfeiter have new technology at hand that makes it possible to design and produce very high quality banknotes easily and quickly. Second, the number of people worldwide with access to technology enabling production of good quality counterfeits has increased by many times. These 'casual' counterfeiters pose a significant threat even though the average number of notes produced per person may be small since the number of potential counterfeiters in this category is very large[1].

Counterfeiting is not a new problem. The barter system used in early societies (which involved the direct exchange of goods) often substituted merchandise of inferior quality or quantity for good products. In later monetary systems using coins of gold or silver, shaving of metal from the coin, hence reducing its value, was common practice. In the U.S. widespread counterfeiting took place around the time of the Civil War leading to some loss of confidence in the currencies in circulation (some issued by private banks) and resulting in adverse economic effects. New engraving and printing techniques were developed and implemented under governmental control (a high tech solution in the 1880's which used an overt feature) and an aggressive enforcement campaign was instituted by the Secret Service. These steps made counterfeiting a marginal problem for many years. In terms of counterfeit notes thought to be in circulation, it remains so today. The issue is the level of a future counterfeit threat.

---

[1] Counterfeit Deterrent Features for the Next-Generation Currency Design, National Research Council, NMAB-472, 1993

Counterfeiting of U.S. currency has an international component because of the dollar's role as a world currency. An estimated 65% of all dollars in circulation are outside the United States, and a substantial portion of the counterfeit currency in circulation is thought to be produced overseas. The U.S. receives substantial benefits from the dollar's international role since the overseas currency pool effectively functions as an interest free loan with an estimated value of $14B per annum to the U.S. treasury. An indirect benefit of the pool is that the economic health of the U.S. and, hence the value of its currency, is important to many overseas who use the dollar as a medium of exchange and a store of value. On the other hand, the widespread acceptance of the dollar outside the U.S. makes the dollar a target for counterfeiting worldwide, broadening the scope of the counterfeiting threat. The international nature of the threat makes defense of the dollar more difficult since data collection channels which exist within the U.S. are not generally available abroad, and the Secret Service and other governmental law enforcement agencies are less able to identify and prosecute illegal activities. One response to this problem among several others is to improve the ability of individuals, both inside and especially outside, the U.S. to authenticate notes.

## 2.0 CURRENCY SECURITY TODAY

For some years the U.S. has used secure, overt features (typically features which are observable visually) to impede counterfeiting of the currency. Two of the most important are the complex engraved patterns intaglio printed on notes and a special cotton-linen currency paper. This paper now contains colored fibers to enhance the distinctive appearance of U.S. currency paper. These features combine to produce a Federal Reserve Note with a feel and appearance that has been difficult to copy. In fact the feel which originates in the intaglio printing process is widely believed to be the first line of defense in person-to-person transfer. The intaglio printing process embosses the paper surface and provides a special three dimensional printing effect on each note in addition to affecting its feel. The security provided by these features is based on controlled access to the printing equipment and paper and to the complex engraving. The high cost of acquiring intaglio printing equipment and engraving expertise (it takes 7 to 10 years to become a journeyman engraver at BEP) has been a strong bar to the counterfeiter, especially the casual variety in the past.

More recently other security features have been added to the currency. Fine lettering is now seen in several locations on the note. This lettering can be read visually but is difficult to photocopy using standard copiers. A second security feature is the overprinting on the Treasury Seal where a second distinct pattern is printed over the pattern written by the intaglio process. In the Treasury Seal example, green ink is overprinted in the seal region and both the green overprint and black intaglio patterns can be seen. Photocopying requires careful color separation a somewhat difficult task on conventional copiers.

These features were adequate to protect the currency from significant levels of counterfeiting for many years. However, with the advances in technology, concern has risen over potential counterfeiting threats and, in response, the Bureau of Engraving and Printing of the U.S. Department of the Treasury has decided to add new security features to the currency. Figure 1 summarizes overt features in the $100 note released in 1996. Intaglio printing, special currency paper and high resolution engraving are still in evidence. In addition, a security thread first added in the 1990 Series is seen. For the new series there is a larger portrait, a watermark, ink that changes color with viewing angle, and microprinting throughout the note and in the thread. The thread also contains a fluorescent phosphor which emits red light under UV illumination.

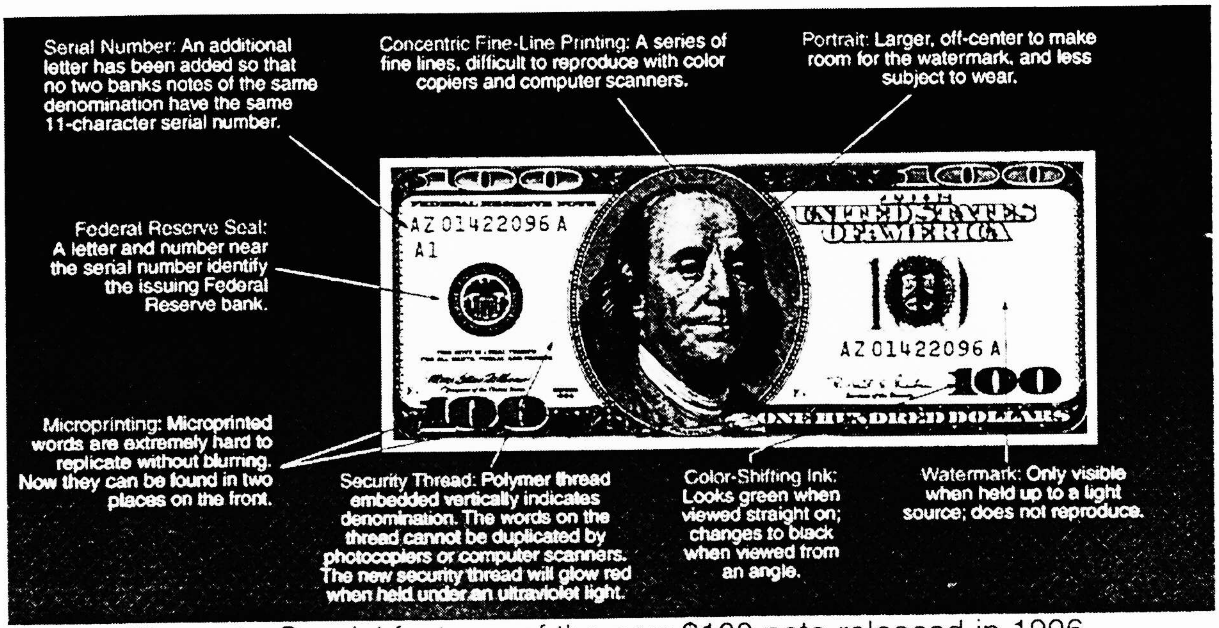
Serial Number: An additional letter has been added so that no two banks notes of the same denomination have the same 11-character serial number.
Concentric Fine-Line Printing: A series of fine lines, difficult to reproduce with color copiers and computer scanners.
Portrait: Larger, off-center to make room for the watermark, and less subject to wear.
Federal Reserve Seal: A letter and number near the serial number identify the issuing Federal Reserve bank.
AZ 01422096 A
A1
UNITED STATES OF AMERICA
AZ 01422096 A
100
100
ONE HUNDRED DOLLARS
Microprinting: Microprinted words are extremely hard to replicate without blurring. Now they can be found in two places on the front.
Security Thread: Polymer thread embedded vertically indicates denomination. The words on the thread cannot be duplicated by photocopiers or computer scanners. The new security thread will glow red when held under an ultraviolet light.
Color-Shifting Ink: Looks green when viewed straight on; changes to black when viewed from an angle.
Watermark: Only visible when held up to a light source; does not reproduce.

Figure 1. Special features of the new $100 note released in 1996.

While the combination of features in the new $100 note, and similar features in other denominations to be issued in the future, are thought to be effective against counterfeiting at this time, it is expected that counterfeiters will try to reproduce the new notes and that it will be necessary to continue development of advanced security features for future series of the currency.

## 3.0 WHO DESIGNS THE CURRENCY?

The simple answer to this question is that a new note is designed by BEP based on such factors as aesthetics, cost, durability and safety. This design is submitted to the Secretary of the Treasury for approval. The approved design is then printed by BEP and sold to the Federal Reserve Bank System hence the name Federal Reserve Note) who issues the notes to banks and the public. In practice the approval process involves at least all of the groups identified in Figure 2. Some participants, such as the Secret Service and the Federal Reserve System are obvious as are suppliers of the specialty papers, inks, printing equipment and inspection equipment used to produce and evaluate the currency. However, there are many other groups who play an important role. A representative list includes such entities as the cash handling and vending industries, metropolitan transportation systems with automated fare transactions and, of course, banks. The public is also consulted using a variety of focus groups since it must accept and use a new design (the Susan B. Anthony dollar coins met significant opposition upon issue and have not been used as expected), as is the Congress, and advocacy groups for people with special needs. The list is long.

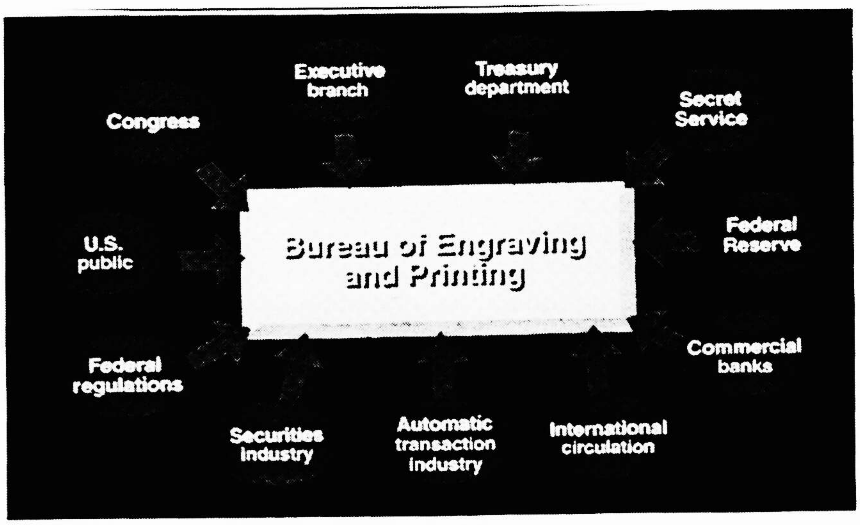

Figure 2. The Bureau of Engraving and Printing receives input from many sources when designing currency.

## 4.0 THE SECURITIES TECHNOLOGY INSTITUTE

The Securities Technology Institute (STI) was founded at the Johns Hopkins University Applied Physics Laboratory in late 1994 by BEP with the charter of identifying techniques for counterfeit detection, identifying or developing counterfeit-deterrence features for the currency, and assessing the threat developments that reprographic and related technology areas pose to the currency in the future. The Institute is working to become a focal point for the science and technology of currency security by establishing relationships with many organizations playing a role in currency security including those named in the previous section. It seeks to develop methods of monitoring developments in reprographic technology and assessing their potential effect on currency security. The Institute is also working to identify and, in some cases, develop security technologies and security features which can authenticate valid notes and identify counterfeit notes. Resources include technical expertise resident at the Johns Hopkins University, individuals in paper and ink industry groups, government technology centers and other expertise found in the printing, reprographic and cash transaction industries.

## 5.0 TECHNOLOGY AND CURRENCY SECURITY

The initial skirmish in the counterfeit wars occurs whenever an attempt is made to put a counterfeit note into circulation. This can be through a person-to-person transfer or a machine transfer, for example at a vending machine. An ideal deterrence feature would authenticate notes for either type of transaction reliably and rapidly enough to prevent the first exchange. Clearly the feature itself must be secure and difficult to counterfeit. For person-to-person transfer overt features are needed. This typically means a specific visual or tactile response. Another possibility could be a distinctive sound produced by the feature which could be recognized by individuals. For machine transactions or machine assisted person-to-person transactions, machine readable features can be used. These can be covert i.e. exclusively machine readable or overt, readable by machine or person. The central issue is feature security. The engraving, special paper and special printing methods used as security features in currency for many years illustrate that overt features can be secure. A metaphor that we have found useful in evaluating approaches to a secure feature is that the Federal Reserve Note is a message sent by the Bureau of Engraving and Printing to those using the currency. The content of the message is that a given note is genuine. This metaphor naturally makes contact with other areas where secure communication is important including military communications in time of war. As expected, the general approaches to security are the same, namely physical security in the form of special apparatus or materials and codes, ciphers or other message-based schemes.

In the currency area one approach is to use materials to write the message that are both unavailable to the counterfeiter and provide a unique response, a kind of high tech "disappearing ink". Typically the approach to developing special materials is through control of chemical composition including development of exotic compounds which are difficult to obtain. However, the iridescent planchettes and in some cases the color shifting inks now used in many currencies point the way to another approach. The response of these materials is determined principally by their structure, that is by the way materials are patterned into a composite structure to provide a unique response to some exciting source based primarily on the structure formed. In the case of planchettes, the structure is a multilayer interference filter where color changes with viewing angle. Another example related by the link of security through structure is use of long chain proteins or DNA strands where the sequence of organic groups along the chains provides a template for attachment of sensing molecules. (For DNA interchain interactions can play a role.) In this example, the structure established by the base pair sequence and pair separation distances controls the response. Knowing the composition without knowing the sequence is insufficient to decode the message. Several general technologies are available to implement this structure controlled response for long chain biomolecules including optical and magnetic response which vary with separation distance. Some concepts based on these types of molecules have been discussed in the literature.[2]

Another approach is to write a coded pattern or sequence on the note. The pattern could be overt or covert. Examples of overt patterns are the holographic, kinographic and other methods of patterning proposed by various groups[3]. These patterns rely on materials and processes to produce pattern and hence fall under the special materials heading. Covert patterns that can rely on codes and can be read only with special probes or by correlation of matched of overt/covert patterns are approaches to security based on secure messaging vs physical security. In this case the metaphor that a secure tag is a secret message sent by BEP to the rest of us is literally correct.

---

[2] New Scientist February 24, 1996 p. 23 "Signed in Blood"

[3] "Optical Document Security", Rudolph L. van Renesse ed., Artech House 1994

A special application area is secure machine readable features used by the Federal Reserve to monitor the pool of circulating currency in the U.S. and to develop currency statistics including counterfeit statistics. One requirement for this application is that the features must be interrogated at high speed. The STI program work in this area spans development of secure sensor concepts and their implementation on the inspection system including hardware, software and signal analysis. A large list of potential technologies which can support secure features has been developed and some specific concepts identified. As expected active and passive optical effects, magnetic effects and acoustic effects are among the technologies under consideration.

## 6.0 SELECTED TAG CONCEPTS

Figure 3 broadly illustrates how a non-contact probe can interrogate a note and "read" a tag. A more practical example is illustrated in Figure 4 where fluorescence from a material in the security thread of a new series $50 or $100 U.S. Federal Reserve Note is monitored. Fluorescence is a very broad approach which can be extended from the response shown in Figure 4 to provide increased security. One extension considers several fluorphores in close enough proximity that Forster type excitation transfer can occur in the excited states of the fluorophores. As a further step the distributions of fluorophores can be spatially patterned to produce sequences of multiple line emission in readable coded sequences. Nonlinear behavior is expected at high fluence levels and provides another extension with presumably higher security.

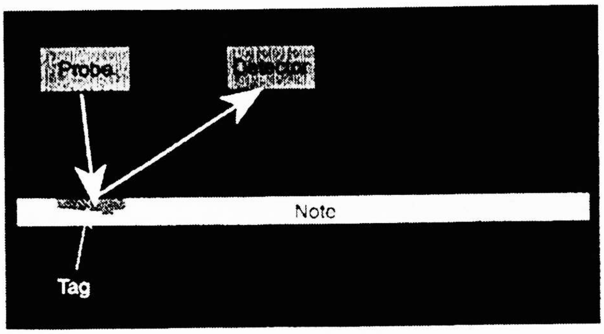

Figure 3. A probe is used to interrogate the note and read the tag (the feature that interacts with the probe). Reading a tag, in effect, is the equivalent of reading a message.

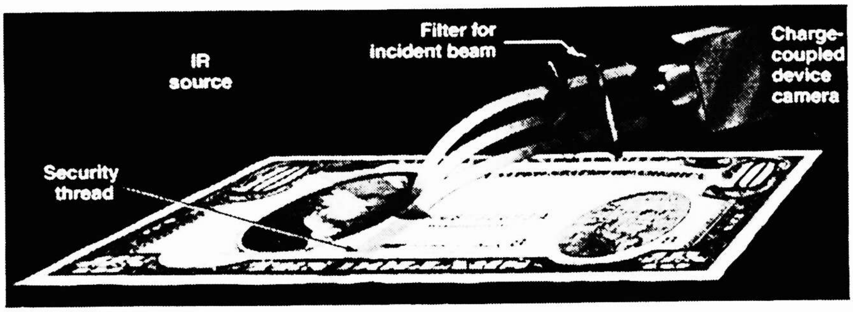

Figure 4. Probing currency using phosphor embedded in security thread.

Acoustic techniques have potential in counterfeit deterrence and are used in the paper industry for on-line product quality control. In the currency authentication area, both noncontact and contact generation and detection of acoustic waves in currency paper is possible. Figure 5a illustrates the generation of acoustic waves in the note by the photoacoustic effect (conversion of heat produced by light absorption into sound). Figure 5c shows an interferometric method of optical detecting the sound at a second location. This combination is a fully optical in - optical out detection approach. However, it is one of several which are available. For example, deflection of a light source by deformation of the note surface provides a way to monitor the acoustic wave propagation. Also, air coupled detection of sound is also possible providing the spectral distribution of the ambient noise is outside the detection region. Figure 5b shows direct coupling of sound from an external acoustic source into a note through a roller system and subsequent detection of the acoustic response at a second set of rollers. Note that a roller system is already present in the current Federal Reserve System inspection machine. Potential security features in acoustic detection depend on the choice of method for generation and detection. In the photoacoustic case, parameters include the light wavelength, the rate of nonradiative relaxation from within the absorbing material and the ratio of thermalization to other methods of relaxation. All these material properties are available for use in a tag.

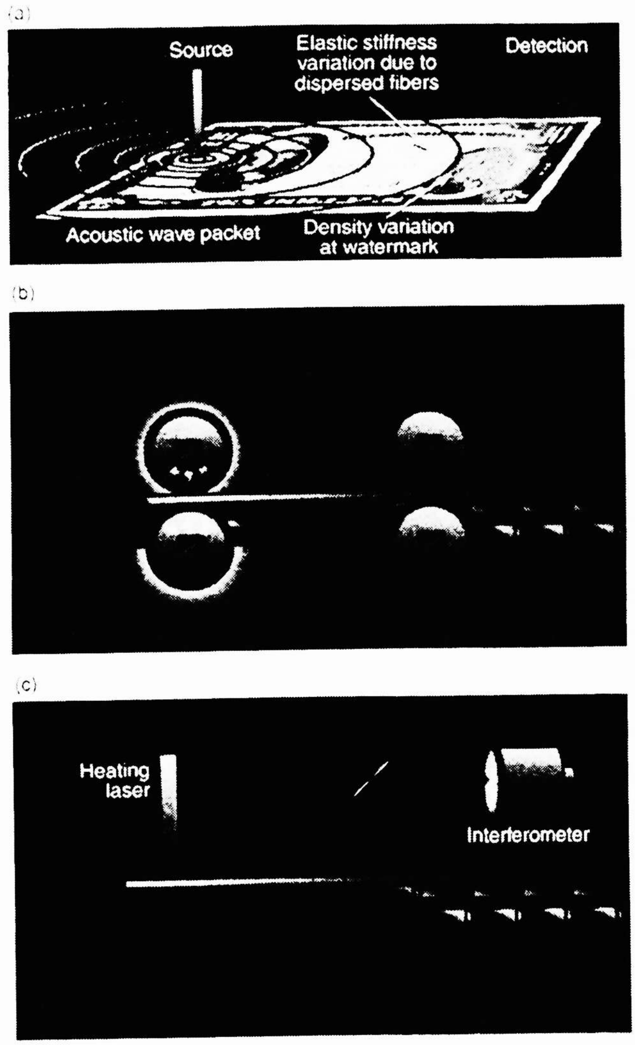
(a)
Source
Elastic stiffness variation due to dispersed fibers
Detection
Acoustic wave packet
Density variation at watermark
(b)
(c)
Heating laser
Interferometer

Figure 5. Probing paper with ultrasound. (a) The velocity of the acoustic waves is determined by the density and elastic stiffness coefficient of the paper. (b) Contact generation and detection using transducers inside fluid-filled rubber wheels. (c) Noncontact thermoelastic generation (laser, microwave).

An independent approach to a secure tag using acoustic methods occurs for propagating acoustic waves in a medium with specific properties. Figure 5b shows a soundwave propagating along the long axis of the note. Typical acoustic velocities for paper are in the range of 200 to 500 meters/second which means that the propagation time through a note 100 microns thick is about 0.3 microseconds and the acoustic propagation time from end to end of the note (15.6 cm) is about 450 microseconds. One concept is to embed at localized sites materials which can generate large amplitude acoustic waves in the paper when illuminated by light. Certain shape memory materials have this property and can be excited by an external stimulus such as temperature as in the photoacoustic effect. Alternatively, these materials can be excited by pressure. Here the roller system could produce waves in the note which could be detected at the second location. By controlling the location of the sound sources spatially coded messages could be produced. Given the large amplitude signals that are possible using shape memory materials it might even be possible to speculate on hearing the sound. Is a note, which when properly excited could say "I'm a hundred!", possible?

Another independent concept is based on distributing small grain size powders of a piezo-electric material on a note either in the substrate or in the ink. For simplicity consider it only in the ink. The initial distribution in orientation of individual powder grains can be modified by an acoustic wave passing through the powder distribution. By the inverse piezo-electric effect passage of a sound wave reorients adjacent grains and produces a kind of periodic grating. This grating can be frozen in place. For example, if the grating is written in the piezo powder while the ink is wet, on drying the powder orientation pattern will remain. To read the pattern a second acoustic pulse of the same frequency and pulse shape is injected into the note. When it interacts with the grating, an acoustic echo is reflected to the sound source. This response occurs only when the frequencies and pulse shape of the write and read waveforms are matched. If multifrequencies are used in the initial pulse, the code written into the powder is detectable only if the interrogating acoustic signal is matched to the original write signal.

## 7.0 SUMMARY

There is a continuing need for the development of secure methods of authenticating currency in person-to-person exchange and in machine transactions. This need is driven by advances in printing, computer and reprographic technology. A metaphor that provides a context for assessment of methods of currency protection is the note as a secure message. The principle issue in any message of this type is security. This can be achieved using either overt or covert features, while for some applications covert features are clearly required. For features based on physical security, a key concept is controlled structure not simply composition.